

Repeaters for continuous-variable quantum communicationFabian Furrer^{1,*} and William J. Munro^{1,2,†}¹*NTT Basic Research Laboratories & Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*²*National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan*

(Received 16 January 2018; revised manuscript received 13 August 2018; published 28 September 2018)

Optical telecommunication is at the heart of today's internet and is currently enabled by the transmission of intense optical signals between remote locations. As we look to the future of telecommunication, quantum mechanics promise new ways to be able to transmit and process that information. Demonstrations of quantum key distribution and quantum teleportation using multiphoton states have been performed, but only over ranges limited to a few hundred kilometers. To go beyond this, we need repeaters that are compatible with these quantum multiphoton continuous-variable pulses. Here we present a design for continuous-variable quantum repeaters that can distribute entangled and pure two-mode squeezed states over arbitrarily long distances with a success probability that scales only polynomially with distance. The proposed quantum repeater is composed from several basic known building blocks such as non-Gaussian operations for entanglement distillation and an iterative Gaussification protocol (for retaining the Gaussian character of the final state), but complemented with a heralded non-Gaussian entanglement swapping protocol, which allows us to avoid extensive iterations of quantum Gaussification. We characterize the performance of this scheme in terms of key rates for quantum key distribution and show a secure key can be generated over thousands of kilometers.

DOI: [10.1103/PhysRevA.98.032335](https://doi.org/10.1103/PhysRevA.98.032335)**I. INTRODUCTION**

Today's society has ready access to more knowledge and information than at any time in our history. A key enabler of this is the internet which is underpinned by the worldwide telecommunications infrastructure. The way we currently process, manipulate, and transmit information is "classical" in nature; however, with recent technological advances new paths are opening that allow us to exploit quantum mechanics and its principles [1–3]. Quantum communication [4] and quantum computation [5,6] are such examples where we can perform certain tasks that are either extremely hard or impossible with our classical hardware. The most mature quantum information technology is known as quantum key distribution (QKD) and is a mechanism to establish secret communication between two remote parties [7,8]. Compared to traditional modern but classical cryptography implementations, it provides provable security based on the law of physics and not on the computational hardness of certain problems. QKD requires a quantum communication channel between the two parties, but does not necessarily require challenging quantum operations necessary for large-scale quantum computers. Consequently, devices for QKD have reached a high degree of experimental maturity with commercial products available [9] and long-time field tests have been conducted under real world conditions [10,11].

The majority of the QKD implementations are realized using weak coherent light or single photons with a discrete variable (DV) encoding such as polarization, path, and

time bin [12]. However, as the traditional telecommunication industry uses intense light fields, there is a possibility of incompatibility if one wants to use the existing network infrastructure for both classical and quantum applications. This can be overcome by using a continuous-variable (CV) encoding into phase-space degrees of freedom [13,14]. Since CV QKD only requires generation of Gaussian states and homodyne detection, it allows technologically simple, efficient, and high-frequency implementations. Regardless of whether DV or CV quantum states of light are used, QKD (and quantum communication in general) are severely limited in their communication distances by the exponential fiber losses [12,15].

Quantum repeaters (QR) are the natural solution to this issue [16,17], as they are considered the quantum analog of signal amplifiers used in the conventional telecommunications industry. Various designs for single photon (DV based encoded) have been proposed in the past decade and their performance extensively studied [12,15,18–20]). The basic individual components for these repeaters have been implemented within a number of experimental efforts, yet their full integration has yet to be achieved.

The continuous-variable quantum repeater case is unfortunately the opposite. The field is still in its infancy as we do not even know whether a continuous-variable quantum repeater (CV QR) is possible using polynomial resources. However, given CV QKD's practical implementation advantages, it seems essential that we determine whether its range limitation of approximately 150 km or less (due to finite-size effects and excess noise) can be overcome using quantum repeaters [14,21]. Further complicating this is the fact that it is well known that a CV QR cannot solely be based on Gaussian

*furrer@eve.phys.s.u-tokyo.ac.jp

†bill.munro@me.com

operations [22] due to the Gaussian entanglement distillation no-go theorem [23–25]. Non-Gaussian (NG) entanglement distillation protocols with subsequent Gaussification have been proposed [26–31] and shown to allow a larger degree of entanglement to be distributed than that expected from direct transmission [31]. A preliminary CV quantum repeater scheme [32] has been proposed (using noiseless linear amplifier [33] based channel purification) that overcomes the exponential EPR fidelity scaling with distance but still scales exponentially in the number of swapping operations. Moreover, their scheme only allows one to extend a channel with already low transmission to a channel with larger distance but the same transmission, meaning a strongly entangled CV state cannot be generated.

In this article, we propose a CV quantum repeater scheme that distributes CV entangled states with arbitrary fidelity and a polynomial scaling in the distance. Our proposal builds on the NG entanglement distillation protocols [28,29] and Gaussification protocols [26,27] supplemented with a heralded NG entanglement swapping operation, which allows one to postpone the Gaussification protocol to the very end of the protocol. This avoids the need to run too many iterations of the Gaussification protocol for which the convergence for practical situations is not known. There are a number of means by which we can analyze the performance of our QR scheme but the most natural here is in terms of CV QKD ranges and rates as this would be one of the first applications of such a repeater. We need to show that it outperforms direct transmission for various distances.

II. STRUCTURE OF THE CV QR AND ITS COMPONENTS

The basic structure of a CV quantum repeater (as illustrated in Fig. 1 and described in its caption) is similar to that used in the DV approach [16,17]. Each repeater station containing CV capable quantum memories performs three types of operations: entanglement distribution (a technique to distribute entanglement between adjacent nodes), entanglement purification (a technique to increase the amount of entanglement shared between the nodes), and entanglement swapping (a technique to increase the range over which the entanglement is shared). However, the entanglement source and the protocols for entanglement distillation (purification) and swapping vary crucially between the CV and DV cases. More specifically, our entanglement source is now a two-mode squeezed state located between the adjacent repeater nodes (rather than a source of Bell pairs of single photons), our purification protocols are non-Gaussian entanglement distillation schemes (rather than simple qubit error detection codes), and our entanglement swapping schemes use homodyne based detection rather than probabilistic Bell state measurements. Further, the CV scheme uses a Gaussification operation to return our distributed entangled state to approximately Gaussian after non-Gaussian operations have been performed on it (for example in entanglement distillation). We store the CV states present in the repeater nodes in our quantum memories when they are not being used for entanglement distillation or swapping. In the next several sections we will describe these CV operations.

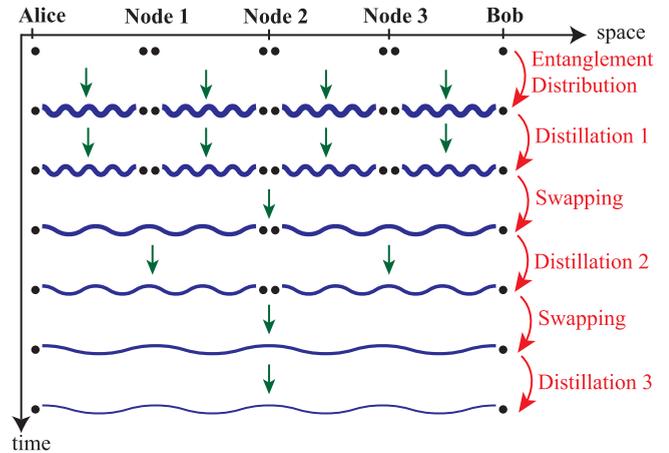


FIG. 1. Schematic illustration of a traditional first generation quantum repeater scheme [15] between Alice *A* and Bob *B*, where that communication distance is divided into shorter distances by adding repeater nodes (stations) in between (three nodes in this case). The repeater scheme begins by establishing entanglement between the adjacent nodes. This entanglement is stored in quantum memories present within each repeater node until we require its use. Then, entanglement distillation (Distillation 1) is performed to distill a smaller number of highly purified and entangled states (number of copies is illustrated by the thickness). Subsequently, entanglement swapping is performed until one established the required entangled state between Alice and Bob. Distillation 2 and Distillation 3 might be necessary to compensate the loss of purity and entanglement during swapping. Instead of using distillation protocols one can utilize a quantum error correction code for the distribution of the entanglement and for the errors induced by the swapping operation.

III. ENTANGLEMENT SOURCE

The most fundamental component of any repeater scheme is the entanglement source depicted in Fig. 2 and for the continuous-variable scheme it is the two-mode squeezed vacuum (also known as the Einstein-Podolski-Rosen (EPR) state [13,34]) depicted in Fig. 2 given by

$$|\chi_\lambda\rangle = \sqrt{1 - \lambda^2} \sum_{k=0}^{\infty} \lambda^k |k, k\rangle. \tag{1}$$

Here $\lambda = \tanh r \in [0, 1)$ determines the strength of the squeezing (with r being the usual squeezing parameter). For $\lambda = 0$, we recover the vacuum, while for $\lambda \rightarrow 1$ we obtain the unphysical infinite energy state where both quadratures are perfectly correlated. Of course, as we need to distribute this entanglement between nodes channel losses are important. Here we will focus on the fully symmetric situation in which the losses for both modes of the entangled EPR states are symmetric, meaning the source is placed in the middle between any adjacent repeater nodes.

An EPR state with losses can conveniently be characterized in terms of its covariance matrix (CM). Because the state is Gaussian and the displacement is zero, this determines the state uniquely. The CM of an EPR state with symmetric losses from transmission of each mode through a channel with

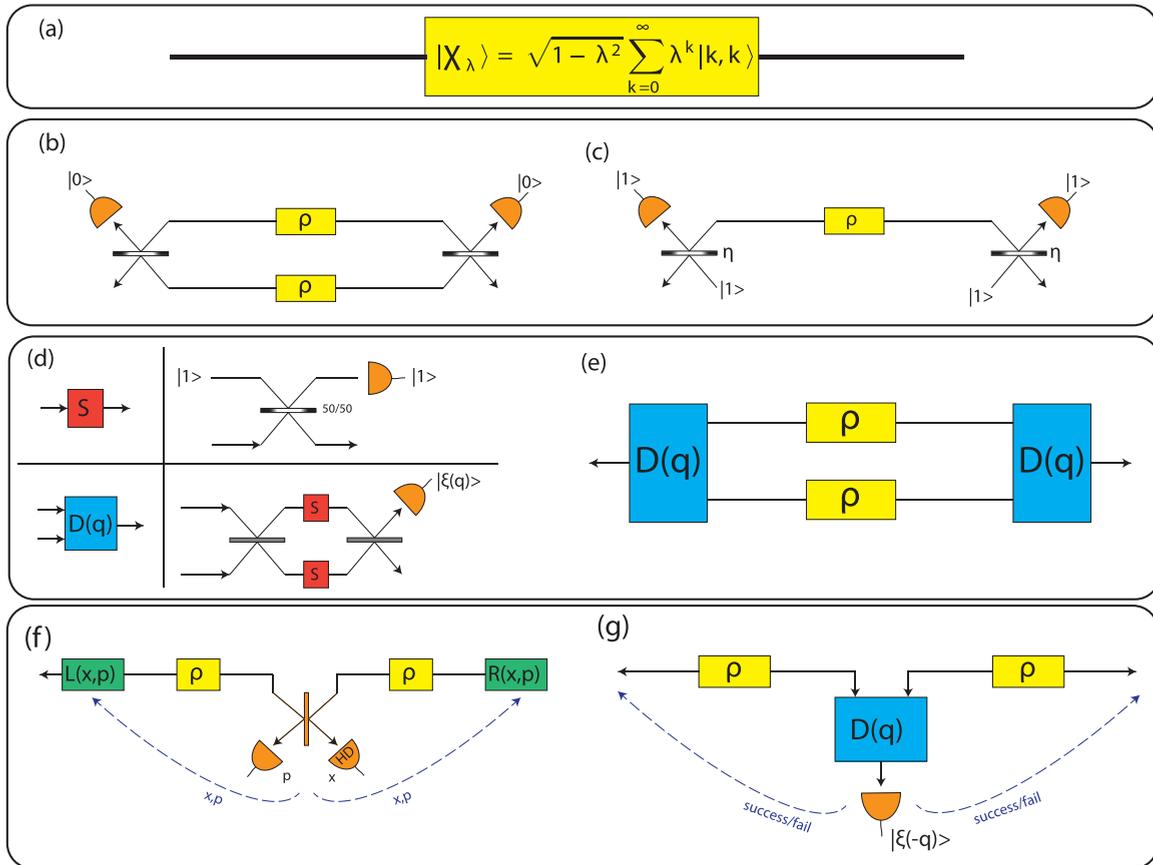


FIG. 2. Schematic illustration of the various CV repeater components. In (a) the two-mode squeezed vacuum entanglement source $|\chi_\lambda\rangle = \sqrt{1-\lambda^2} \sum_{k=0}^{\infty} \lambda^k |k, k\rangle$ is depicted. In the important Gaussification protocol s is shown which transforms non-Gaussian states back to Gaussian ones. On both nodes, the two modes are mixed with a balanced 50:50 BS. The operation succeeds conditioned on vacuum port detection (a Gaussian filtering operation) at both nodes. This procedure can be iteratively executed with the obtained state as the new input state until one is close enough to the desired Gaussian state. By choosing different filtering operations [31] different Gaussification protocols are obtained. In (c) the symmetric PR distillation protocol is depicted where both modes are mixed with a single photon using a BS with transmissivity η . The operation is successful if a single photon is measured at the respective outcome of the BS. Panel (d) shows the operations S and $D(q)$ used in the purifying distillation protocol. Here S is a photon replacement with a balanced BS, while $D(q)$ is a probabilistic operation consisting of a Mach-Zehnder interferometer with S placed in each path and conditioning on $|\xi(q)\rangle$ on one of the output ports. Next (e) illustrates the purifying distillation operation in which $D(q)$ is applied to two initial states ρ . Heralding is applied on the successful application of $D(q)$ on both sides. The usual Gaussian entanglement swapping protocol S is shown in (f), where the two modes are mixed with a balanced BS and homodyne detection (HD) is used on both output ports to measure X and P . A correction operation in the form of a displacement depending on the measurement outcomes is applied on the left and right mode. Finally (g) shows a NG entanglement swapping protocol. The operation is heralded upon success of the operation $D(q)$ and measuring the state $|\xi(-q)\rangle$.

transmissivity τ (losses $1-\tau$) has the form

$$\Gamma = \begin{pmatrix} C\mathbf{I} & SZ \\ SZ & C\mathbf{I} \end{pmatrix}, \quad (2)$$

where $Z = \text{diag}(1, -1)$, $C = 1 + \tau[\cosh(2r) - 1]$, and $S = \tau \sinh(2r)$. Next let us examine the protocols required for entanglement distillation and swapping.

IV. GAUSSIFICATION PROTOCOL

Our entanglement distribution process uses Gaussian states that retain this Gaussian nature even under loss. However, some of our entanglement distillation protocols result in non-Gaussian states being formed and so the resulting NG states can no longer be fully described by the CM. Instead we need a different parametrization. It is useful to use the matrix

coefficients of the state in the photon number basis. For any two-mode state ρ , we denote the matrix elements in the number basis by $\rho_{kl,\alpha\beta} = \langle k, l | \rho | \alpha, \beta \rangle$, where $\{|n\rangle\}$ denotes the number basis of a single mode. A lossy EPR state satisfies the constraints

$$\rho_{kl,\alpha\beta} = \rho_{lk,\beta\alpha}, \quad (3)$$

$$\rho_{kl,\alpha\beta} = 0, \quad \text{if } k - \alpha \neq l - \beta, \quad (4)$$

$$\rho_{kl,\alpha\beta} \in \mathbb{R}, \quad (5)$$

where the explicit form of the coefficients for low photon numbers can be found in [28]. It is important that this NG state can be made more Gaussian in nature as we attempt our long CV entanglement generation process, which is where the

Gaussification protocols come into play [26,27,30,31]. Let us examine this in more detail.

Consider that our initial resource state is given by the two-mode state ρ^0 , where the two modes are at two spacelike separated nodes N and M . Then, in the first iteration of the Gaussification protocol [see Fig. 2(b)] two resource states $\rho^0 \otimes \rho^0$ are used to generate a two-mode state ρ^1 on N and M in a probabilistic but heralded fashion. In the second iteration, the same procedure is applied with the resource state ρ^1 . Hence, from $\rho^1 \otimes \rho^1$, a two-mode state ρ^2 is generated. In the limit of infinite iterations $i \rightarrow \infty$ one obtains a Gaussian state ρ^∞ , whose form for the CM has been shown in [30,31].

The characterization of the CM is simple if the low photon matrix in the Kronecker basis $\{|0, 0\rangle, |0, 1\rangle, |1, 0\rangle, |1, 1\rangle\}$ $F_1(\rho^0) := (\rho_{kl,\alpha\beta}^0)_{k,l,\alpha,\beta=0}^1$ has the form

$$F_1(\rho) = \begin{pmatrix} \rho_{00,00} & 0 & 0 & \rho_{11,00} \\ 0 & \rho_{01,01} & 0 & 0 \\ 0 & 0 & \rho_{01,01} & 0 \\ \rho_{11,00} & 0 & 0 & \rho_{11,11} \end{pmatrix}. \quad (6)$$

which is certainly the case for the symmetric EPR state (3)–(5). Then, the CM is determined by the low photon number matrix $F_1(\rho)$ only and the CM of the corresponding Gaussified state has the same form as an EPR state with symmetric losses (2). In order to express the CM in terms of $\rho_{kl,\alpha\beta}$ it is convenient to introduce the quantities

$$\varepsilon(\rho) = \frac{\rho_{10,10}}{\rho_{11,00}}, \quad \Lambda(\rho) = \frac{\rho_{11,00}}{\rho_{00,00}}. \quad (7)$$

The CM of ρ^∞ is then given by (2) with [28]

$$C = \frac{\Lambda^2(1 - \varepsilon^2) + 1}{(1 - \varepsilon\Lambda)^2 - \Lambda^2}, \quad S = \frac{2\Lambda}{(1 - \varepsilon\Lambda)^2 - \Lambda^2}, \quad (8)$$

where $\varepsilon = \varepsilon(\rho)$ and $\Lambda = \Lambda(\rho)$. We need to point out explicitly that there exists states ρ for which the obtained CM is not physical, that is, it does not satisfy the necessary condition $\Gamma + i\Omega \geq 0$ with Ω the symplectic form [13]. In this case, the Gaussification protocol does not converge. We can now invert our expressions $C = 1 + \tau[\cosh(2r) - 1]$ and $S = \tau \sinh(2r)$ from Eq. (2) to express the state ρ^∞ as a lossy EPR state with squeezing parameter $\lambda = \lambda_\infty(\rho)$ and symmetric transmissivity $\tau = \tau_\infty(\rho)$ given by

$$\lambda_\infty(\rho) = \varepsilon(\rho) + \Lambda(\rho)[1 - \varepsilon(\rho)^2], \quad (9)$$

$$\tau_\infty(\rho) = [1 - \varepsilon(\rho)^2]\Lambda(\rho)/\lambda(\rho), \quad (10)$$

which yields [28]

$$\varepsilon(\rho) = \lambda_\infty(\rho)[1 - \tau_\infty(\rho)]. \quad (11)$$

Finally, although we make a strong distinction between NG entanglement distillation and Gaussification, we emphasize that generally the Gaussification protocol also increases the entanglement of the input state. NG entanglement distillation is however much more efficient than Gaussification and so let us turn our attention to such protocols.

V. ENTANGLEMENT DISTILLATION AND PURIFICATION PROTOCOLS

Entanglement distillation is the process by which we can take several copies of the quantum state and operate on them to obtain a new quantum state with increased entanglement. We are now going to examine two distillation protocols that are both based on a probabilistic approach in which the desired states are distilled by conditioning on a suitable measurement outcome. The first one called symmetric photon replacement (PR) [26,27] has the ability to efficiently increase the entanglement of the resulting state, but not its purity [29]. The second protocol called purifying distillation overcomes this problem and allows one to purify the state arbitrarily [29]; however, it has the disadvantage that the success probability is very low and its implementation is much more demanding.

It is necessary at this stage to mention how we are going to characterize the states ρ resulting from the entanglement distillation and purification protocols. We have many choices available including a number of entanglement measures but as our overall aim is the generation of remote long-range EPR states, we can consider the Gauss parameters $\lambda_\infty(\rho)$ and $\tau_\infty(\rho)$, which would be the state we get after many rounds of Gaussification. In a real sense this indicates how the squeezing parameter and symmetric transmissivity have changed due to the distillation and purification protocols. It may be indirect in nature, but it is our choice here.

A. Symmetric photon replacement distillation

The starting point for this distillation procedure shown in Fig. 2(c) is a two-mode state ρ shared between two nodes N and M . In the symmetric PR distillation protocol, both modes are mixed at a beam splitter with transmittance η with a single photon. The output port of the single photon is then measured with a single photon detector. The operation is successful if on both modes a single photon is detected and the corresponding output state is denoted by $\tilde{\rho}$.

At this stage we need to be able to characterize how effective our distillation has been. As shown in [28], the symmetric PR distillation can be characterized by

$$\varepsilon(\tilde{\rho}) = \varepsilon(\rho), \quad (12)$$

$$\Lambda(\tilde{\rho}) = \beta(\eta)^2 \Lambda(\rho), \quad (13)$$

where $\Lambda(\rho) = \rho_{11,00}/\rho_{00,00}$ and $\beta(\eta) = (2\eta^2 - 1)/\eta$. By tuning η the Gauss parameter $\tilde{\lambda}_\infty$ can be made arbitrary close to 1 but at the expense of decreasing the success probability. Care also needs to be taken to ensure that η is not chosen such that $\Lambda_\infty(\tilde{\rho}) > 1/(1 + \epsilon)$; otherwise, $\tilde{\lambda}_\infty > 1$, which is unphysical (further it means that the Gaussification protocol will no longer converge). Now since the low photon matrix of a symmetric EPR state has the form (6) and it is conserved by the symmetric photon replacement (and all operations considered in here), the Gauss parameters provide a handy tool to characterize the effect of the distillation. It also enables us to define $\varepsilon(\rho) = \lambda_\infty(\rho)[1 - \tau_\infty(\rho)]$, which turns out to be equal to $\varepsilon(\rho) = \langle 1, 0 | \rho | 1, 0 \rangle / \langle 1, 1 | \rho | 0, 0 \rangle$ [28]. The symmetric photon replacement has now the simple property that $\varepsilon(\tilde{\rho}) = \varepsilon(\rho)$ [28].

However, as pointed out in [29], any operation that leaves ε invariant cannot increase the purity of the state. In order to increase the purity ε has to be decreased. Hence the disadvantage of symmetric PR distillation is that it will always decrease the purity of the resulting state [29] as it increases entanglement. This can cause a problem for a CV QR as, for instance, subsequent application of entanglement swapping reduces the purity. For instance, with the symmetric PR distillation alone, we are not able to show that our CV QR scales for all distances only polynomial in the distance.

B. Purifying distillation

As the name suggests the purifying distillation protocol introduced in [29] overcomes the problem of the symmetric PR distillation protocol and allows us to increase the purity of the state. It however requires two two-mode states ρ as a resource in order to distill a two-mode state $\tilde{\rho}$ that has higher purity. The structure of the protocol depicted in Figs. 2(d) and 2(e) consists of a NG operations $D(q)$ performed on the two copies of the state ρ . The core operation $D(q)$ consists of a Mach-Zehnder interferometer in which a probabilistic NG operation S is placed in both paths followed by a measurement projection onto the state

$$|\xi(q)\rangle = \frac{1}{\sqrt{1+q^2}}(q|0\rangle + |1\rangle) \quad \text{with } 0 \leq q \leq \infty. \quad (14)$$

Such a measurement can be implemented by displacements and photon addition together with projecting on the vacuum [35]. Next critical to this $D(q)$ operation is the choice of S and in this case we choose a photon replacement operation with a balanced BS [see Fig. 2(d)] due to its easy experimental implementation. This operation has the mathematical form

$$S = \frac{1}{\sqrt{2^{\hat{n}+1}}}(\hat{n} - 1), \quad (15)$$

with \hat{n} denoting the number operator and filtering out the single-photon components. This approximates the operation $\hat{n} - \mathbb{1}$ originally proposed by [29] up to a factor depending on the photon number. The idea behind this choice is that it maps up to a phase $\langle 0|$ and $\langle 1|$ in the Heisenberg picture to $\langle 00|$ and $\langle 11|$, because the states $\langle 01|$ are filtered out by the Mach-Zehnder interferometer if in both arms the single-photon events are filtered out. This has the consequence that $\tilde{\rho}_{ik,\alpha\beta} \sim \rho_{ik,\alpha\beta}^2$, which implies that $\varepsilon(\tilde{\rho}) = \varepsilon(\rho)^2$. Hence, since ε is smaller than 1, ε decreases, which leads to Gauss parameters corresponding to a Gaussian state with increased purity (see the Appendix for further details).

The implementation of $D(q)$ is more complicated than symmetric photon replacement distillation as it requires PR to be implemented twice within each repeater node as well as the measurement based projection onto the state (14). Further the success probability of the purifying protocol is much lower than PR. In particular, higher-order photon terms are strongly suppressed. To illustrate this we plot in Fig. 3 the success probability of the purifying distillation as well as the Gauss parameter for the output transmissivity.

VI. ENTANGLEMENT SWAPPING PROTOCOLS

We have now established entanglement distribution and distillation protocols for our CV quantum repeater scheme. The final protocol required is entanglement swapping, which allows us to extend the range of our entanglement beyond what we can create between adjacent repeater nodes. Here two main swapping options are possible: Gaussian entanglement swapping and non-Gaussian entanglement swapping [see Figs. 2(f) and 2(g)].

A. Gaussian entanglement swapping protocols

If the initial states are lossy EPR states one can simply choose the standard Gaussian swapping protocol [36] based on Gaussian teleportation [37–39]. In such a case the two modes at the same node are mixed with a balanced BS, whereupon homodyne detection is used to measure the X amplitude of one output and the P amplitude of the other output [see Fig. 2(f)]. The measurement outcomes are then sent to the other nodes and a corresponding correction operation in the form of a displacement is made. Given that the outcomes of the X and P measurement are x and p , the displacement on the left mode is $g\sqrt{2}(-x + ip)$ and on the right mode $g\sqrt{2}(x + ip)$, where g is the gain that has to be adjusted [36]. It is now critical to mention that these displacements are likely to increase the proportion of two photons moving us out of the subspace we preferred for the entanglement distillation.

B. Non-Gaussian entanglement swapping protocols

There is a potential issue with using the conventional Gaussian entanglement swapping operation. Before the Gaussian entanglement swapping can be applied, a Gaussification protocol has to be used to turn the NG state after entanglement distillation again into or close to a lossy EPR state. But since the above distillation protocols suppress the higher photon number components, several iterations might be required to retain the state's Gaussian character. This is especially a problem if one wants to distill a highly entangled state. An alternative NG entanglement swapping protocol is possible that does not require the Gaussification step [see Fig. 2(f)].

The idea is to swap the entanglement in the low photon number subspace spanned by the local one photon subspaces. For simplicity, let us consider the case with no losses, where the projection of an EPR state onto the local one-photon subspace is up to normalization given by $|\tilde{\chi}_\lambda\rangle = |00\rangle + \lambda|11\rangle$ [see Eq. (1)]. The tensor product is simply

$$|\tilde{\chi}\rangle_{12} \otimes |\tilde{\chi}\rangle_{34} = |00\rangle_{14}|00\rangle_{23} + \lambda^2|11\rangle_{14}|11\rangle_{23} + \lambda(|01\rangle_{14}|01\rangle_{23} + |10\rangle_{14}|10\rangle_{23}), \quad (16)$$

where modes 2 and 3 are assumed to be at the same node. Hence, in order to swap the entanglement, we have to project modes 2 and 3 onto a state proportional to $|\tilde{\chi}_a\rangle$ to obtain

$$|00\rangle + a|11\rangle. \quad (17)$$

Now letting $a = 1/\lambda$ we perfectly swapped our initial truncated EPR states. In order to realize a projection onto a state $|\tilde{\chi}_a\rangle$ with experimentally feasible operations, we need to cut out the components $|01\rangle, |10\rangle$. However, as we have

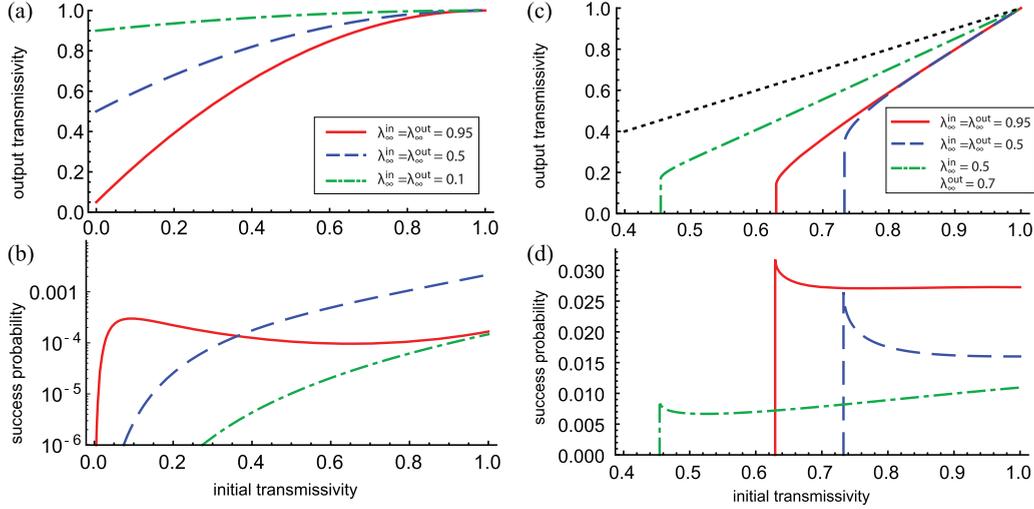


FIG. 3. Plot of the Gauss parameter for the transmissivity of the output state $\tau_\infty(\bar{\rho})$ and the corresponding success probability p_{succ} depending on the Gauss parameter for the transmissivity of the input state $\tau_\infty(\rho)$. In (a),(b) we illustrate the purifying distillation situation where our projective measurement $|\xi(q)\rangle$ has the free parameter q depending on the choice of state on which we wish to condition. We can tune q such that the Gaussian parameter for the input squeezing $\lambda_\infty^{\text{in}} = \lambda_\infty(\rho)$ and output squeezing $\lambda_\infty^{\text{out}} = \lambda_\infty(\bar{\rho})$ are equal but $\varepsilon(\bar{\rho}) < \varepsilon(\rho)$, that is, $\bar{\rho}$ is more pure than ρ . In (c),(d) we consider the non-Gaussian entanglement swapping situation. The Gaussian parameters for the input squeezing $\lambda_\infty^{\text{in}} = \lambda_\infty(\rho)$ and output squeezing $\lambda_\infty^{\text{out}} = \lambda_\infty(\bar{\rho})$ are shown. In order to illustrate the decrease of the Gauss output transmissivity parameter (c), we also plotted the input transmissivity (dotted line). We see that there exists a minimal initial transmissivity for the protocol to conserve the desired structure of the input state (i.e., the Gaussification protocol converges). The success probability increases and the threshold for the initial transmissivity gets reduced for larger squeezing $\lambda_\infty^{\text{in}} = \lambda_\infty^{\text{out}}$. The threshold for the initial transmissivity is also reduced if the output squeezing $\lambda_\infty^{\text{out}}$ is larger than initial squeezing $\lambda_\infty^{\text{in}}$, but the success probability decreases.

seen in Sec. VB this can be achieved by a Mach-Zehnder interferometer with photon replacement in the two paths, that is, an operation similar to $D(q)$. Indeed, a straightforward computation shows that

$$D(q)^* |\xi_{\bar{q}}\rangle = \frac{q\bar{q}|00\rangle - 1/4|11\rangle}{\sqrt{2(1+q^2)(1+\bar{q}^2)}}. \quad (18)$$

Hence, by choosing $\bar{q} = -q$ we obtain the projection on a state proportional to $|\tilde{\chi}_a\rangle$. This motivates our choice of the NG swapping operation consisting of an application of $D(q)$ followed by condition on the state $|\xi_{-q}\rangle$ as illustrated in Fig. 2(g). It is important to mention that this new NG swapping protocol is not deterministic and the information whether or not it succeeded has to be communicated to the other nodes. This is in contrast to the Gaussian entanglement swapping, which is deterministic.

We can now characterize the effect of the NG swapping protocol on a state ρ . By using (18) the resulting state $\bar{\rho}$ in matrix form is given by

$$\begin{aligned} \bar{\rho}_{i,j,\alpha\beta} = & \frac{1}{2(1+q^2)^2} \left(q^4 \rho_{i0,\alpha0} \rho_{0j,0\beta} + \frac{1}{4} \rho_{i1,\alpha1} \rho_{1j,1,\beta} \right. \\ & \left. + \frac{q^2}{2} (\rho_{i0,\alpha1} \rho_{0j,1\beta} + \rho_{i1,\alpha0} \rho_{1j,0\beta}) \right), \end{aligned} \quad (19)$$

where the free q parameter can be adjusted to give the desired Gauss squeezing parameter λ_∞ . In Fig. 3 we plot the success probability and Gauss output transmissivity parameter for different values of the Gauss parameters for the input squeezing and the output squeezing. We observe that there exists a threshold for the input Gauss transmissivity parameter $\tau_\infty(\rho)$ below which the operational interpretation of the Gauss

parameters fails, that is, the Gaussification of the output state does not converge any more. According to Fig. 3, this threshold crucially depends on the Gauss parameter for the initial and final squeezing. More precisely, if the Gauss parameter for the output squeezing is larger than the input squeezing, a lower Gauss parameter for the transmissivity is possible. But at the same time this decreases the success probability of the NG swapping protocol as well as the purity of the output state.

VII. CV QUANTUM REPEATERS

We now have all the components (entanglement distribution, entanglement distillation, and entanglement swapping) required to design and quantitatively analyze how a CV quantum repeater would work. We do however need to specify a figure of merit for its performance. This will obviously depend on the application, but as a natural first step we will estimate the secret key rate if the distributed state had been used for CV QKD using a homodyne based detection scheme [14]. Here we are actually generating the entangled state between the two end nodes of the repeater before it is measured for QKD.

A. Polynomial scalings

The key step for our CV quantum repeater scheme is to show that in principle it can overcome the exponential decay of the entanglement generation rate, rather than worrying initially about whether the performance is optimal or not. In principle one needs to show that the EPR generation rate and resources consumed scales polynomial with the total communications distance (others sometimes use the definition that the CV repeater EPR generation rate should beat that

associated with direct transmission but we avoid this as it is well known that some QKD schemes which are not repeaters already exceed that).

Consider that the total distance we want to establish our key over is L and it is divided into 2^n equal segments each of length $l = L/2^n$ with a repeater station joining each segment. In total we have $N = 2^n - 1$ repeater stations (excluding the end points) and N swapping operations are required. Since we are examining a symmetric QR protocol, the source is placed in the middle between any two adjacent repeater stations and so the initial transmittance of each mode is $\tau_0 = \tau(l/2)$. We fix the final squeezing λ_{final} and transmittance τ_{final} of the target EPR state we want to distribute between the end nodes.

Our scheme, as depicted in Fig. 1, begins with the distribution of the EPR state between adjacent nodes. Once this has been successful, we apply entanglement distillation protocols (symmetric PR and purifying distillation) to generate a state that has Gauss parameters that are at least those of the desired target state. The success probability p_0 of the initial distillation depends on the initial squeezing and the distance between adjacent nodes l and is thus independent of the total distance. Subsequently, entanglement swapping is applied. Here we have two situations depending on whether we use Gaussian or non-Gaussian entanglement swapping protocols.

Gaussian approach. In this situation we need to perform Gaussification after each entanglement distillation step before entanglement swapping can be performed. The success probability p_{dist} for the entanglement distillation can also incorporate the success probability for the Gaussification operation. The Gaussian entanglement swapping is deterministic so $p_{\text{swap}} = 1$.

NG approach. The non-Gaussian entanglement swapping operation succeeds with probability p_{swap} , which depends on the Gauss parameter of the input state (i.e., determined by the target state). Gaussification is not required in this case before the NG swapping is performed. Another round of entanglement distillation is used to retain again a state that complies with the target state. The success probability p_{dist} for the entanglement distillation only depends on the properties of the NG swapping protocol and the squeezing and transmittance of the target state.

In the same way NG swapping and entanglement distillation can simply be applied as many times as required to reach the desired distance L . Hence we find that the rate associated with distillation and swapping operations scales with $(p_{\text{swap}} p_{\text{dist}})^n = (p_{\text{swap}} p_{\text{dist}})^{\log_2(L/l)}$ [40], which is polynomial (and not exponential) in the total communications distance L . It is important to mention here that this scaling is not p_{swap}^N as many of the swapping operations can be attempted in parallel [41]. Finally, the Gaussification protocol is applied to generate an approximate Gaussian state with the squeezing and transmittance. Given that the success probability for the Gaussification protocol is p_{Gauss} , we find that the overall rate for generated CV entangled links between the end nodes is

$$R = \frac{2L}{c} p_0 p_{\text{Gauss}} \left(\frac{L}{l} \right)^{\log_2(p_{\text{swap}} p_{\text{dist}})}, \quad (20)$$

which scales polynomially in the total distance L , where c is the speed of light in the channel. The average number

of EPR required to generate the long-range EPR is then $N_{QR} \sim (L/l)^{\log_2(2\alpha^*) - \log_2(p_{\text{swap}} p_{\text{dist}})} / p_0 p_{\text{Gauss}}$ remembering that two EPR pairs are required entanglement swapping attempts and α^* per distillation attempt ($\alpha^* = 1$ for symmetric PR distillation; 2 for purifying distillation and Gaussification). The normalized generation rate (raw rate/EPR pairs used) is then given by $R_{QR} = R(\rho_{\text{target}})/N_{QR}$, where ρ_{target} denotes the target state. We need to remember here for the Gaussian entanglement swapping operation $p_{\text{swap}} = 1$ but p_{dist} also includes the probabilistic nature of the Gaussification operation. Finally, in this in principle approach, we have performed entanglement distillation at every round. This is unlikely to be necessary and the removal of a few rounds of these should dramatically improve performance as the success probability for the purifying distillation p_{dist} is quite low (see Fig. 3). It will not change the overall scaling from polynomial to exponential.

B. CV quantum key distribution

In order to keep the calculation of the key rate simple we use the asymptotic key rate formula that is uniquely determined by the CM of the distributed state [13,14,42]. This ignores finite-size effects. It is important to note that the state does not have to be a Gaussian state in order for the key rate formula to apply due to the extremality property of Gaussian states [43,44]. Moreover, in [45] it has been shown how the CM can be estimated without assuming the state is Gaussian.

To begin let us examine how the key rate can be computed without CV QR restricting ourselves for simplicity to only collective attacks. If the input state is independent and identically given by ρ , the key rate in the asymptotic limit is [42,46]

$$r(\rho) = I(X_A : X_B)_{\rho^G} - I(X_B : E)_{\rho^G}, \quad (21)$$

where ρ^G denotes the Gaussian state with the same second moments as ρ , $I(X_A : X_B)_{\rho^G}$ the mutual information of Alice's and Bob's key generating measurement applied to the Gaussian state, and $I(X_B : E)_{\rho^G}$ the mutual information (or Holevo quantity) between the eavesdropper and Bob's measurement. We emphasize that the key rate above is for the case of reverse reconciliation, which is favorable for high losses. $r(\rho)$ can then be applied to calculate the key rate for direct transmission. For that, we choose ρ as an EPR state where one mode is sent through a fiber channel with transmittance $\tau(l) = 10^{-l\mu/10}$, where l is the channel length and μ the loss per kilometer (set to 0.2 km in the case). For an asymmetric loss distribution using reverse reconciliation [47], the key rate for CV QKD decreases linearly with the transmittance, and thus exponentially with the distance. This expression also gives us a direct way to compare our repeaters performance. In addition, we can also compare our scheme against the upper bounds for direct transmission determined by [48] which decrease linearly with the transmittance and exponentially with the distance.

For our CV quantum repeater protocol the distributed entangled states are symmetric in nature rather than the optimal asymmetric loss distribution used in the original CV QKD. This has the consequence that a positive key rate cannot be obtained for low losses and an EPR state with relatively high

transmissivity is required. In order to compute this key rate, let us assume that we distribute the state σ using a CV QR. Then, the key rate associated with the CV QR is then

$$r_{\text{QR}}(\sigma) = \frac{1}{N_{\text{QR}}(\sigma)} r(\sigma), \quad (22)$$

where $N_{\text{QR}}(\sigma)$ denotes the average number of initial EPR states that are consumed to distribute the state σ with the CV QR. The normalized key rate $r_{\text{QR}}(\sigma)$ is the important quantity to analyze the practicality under finite-size effects and excess noise due to the homodyne detection. However, if $r_{\text{QR}}(\sigma)$ is sufficiently large, this means that even under finite-size effects and additional noise a positive key rate can be obtained. In fact, for direct transmission the key rate $r(\rho)$ gets so low for distances above about 150 km that under practical conditions a positive key rate is no longer currently possible [14,21].

In terms of our CV repeater design we now have a number of choices for how we perform both the entanglement distillation and swapping operations. We will begin by examining Gaussian entanglement swapping based approaches.

C. Gaussian entanglement swapping based CV QR

While the scaling of our CV repeater scheme has been established in a simple fashion, determining its performance requires us to make assumptions about our physical devices and their imperfections beginning with the Gaussian entanglement swapping based CV QR. A similar protocol has been considered in [31], where it has been shown that it allows one to distribute entanglement over longer distances than with direct transmission. However, the success probability of those involved protocols have been neglected.

Now let us begin our analysis of the Gaussian entanglement swapping based CV QR. For simplicity, we will consider an ideal system here where our only source of error are losses in the channel and assume perfect quantum memories, single photon sources and detectors with unity detection efficiency of and zero dark counts. Further in our analysis we will ignore finite-key scale effects. Beginning the analysis it is beneficial due to the channel losses to first distribute a very weakly entangled state and then use symmetric PR distillation to increase its entanglement. Moreover, in order to avoid multiple applications of the Gaussification protocol one wants to apply only entanglement distillation right after the distribution. Every additional intertwined entanglement distillation step would also require an additional Gaussification step. This leads to two difficulties in computing the performance of the CV QR: First, we have to compute the state as well as the success probability that is obtained after a number of iterations of the Gaussification operations. Using the Fock basis to parametrize the state is not suitable to do and the computation is very inefficient. Second is the difficulty to characterize the effect of the Gaussian entanglement swapping protocol on only approximate Gaussian states after a fixed number of Gaussification operations. In particular, the essential structure that allows us to characterize states through their Gauss parameters is no longer conserved. We avoid these problems and simply (over)estimate the performance of the CV QR in Fig. 4 by using the success probability if only three iterations of the Gaussification protocol are executed and calculate the

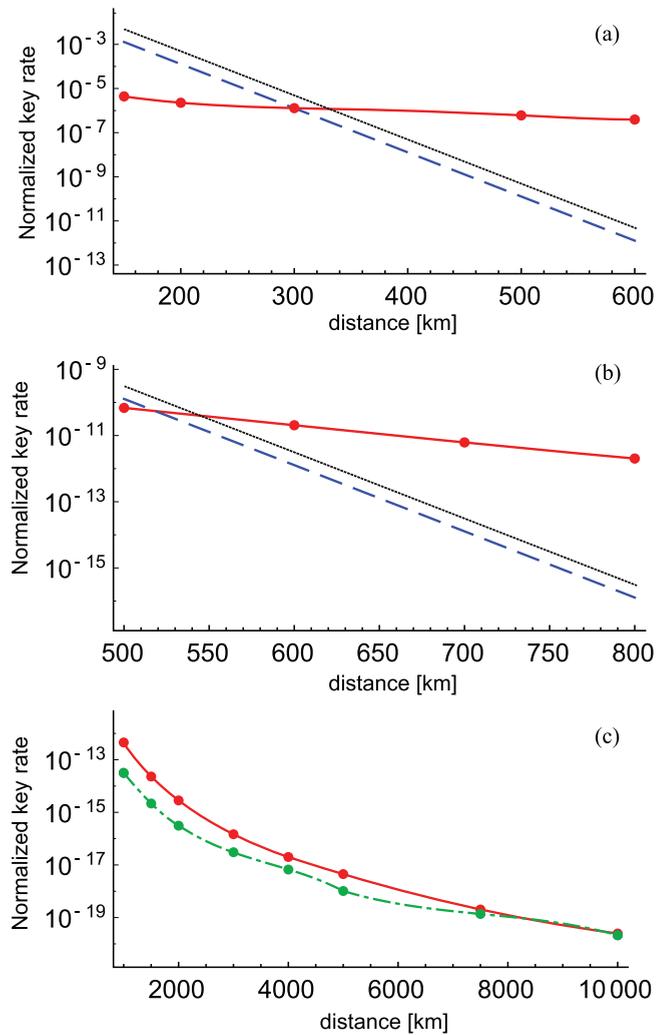


FIG. 4. (a) Plot showing the characteristic behavior of the normalized key rate per pulse $r_{\text{QR}}(\sigma)$ obtained with a CV QR based on Gaussian swapping. The rates are (over)estimated and computed under the simplification that three iterations of the Gaussification protocol would lead to a perfect Gaussian state. (b) Plot showing the performance of the CV QR based on NG entanglement swapping. Shown is the comparison of the estimate key rate or pulse for the CV QR (straight) with the key rate for direct transmission (dashed) using a CV reverse reconciliation scheme [47] and a tight upper direct transmission bound (dotted) [48]. We see that the crossing point is slightly above 350 km (500 km) for the Gaussian swapping (NG swapping) and the gap increases fast with the distance. (c) The lower plot compares the key rate or pulse of the CV QR without (straight) and with (dashed) additional purifying entanglement distillation. We observe that, while for low distances the key rate without additional purifying distance is significantly larger, the gap closes for large distances above 10 000 km. The dots correspond to actual simulation points and the curves are interpolations.

Gaussian swapping for an exact Gaussian state corresponding to the Gauss parameters. We emphasize that this approximation seems rather rough. In fact, the computation shows that after three iterations of the Gaussification protocol the state is still quite far from the corresponding Gaussian state. This clearly overestimates the CV QR rate significantly which

is why we emphasize that it is problematic to compare the actual key rate value with the one using NG entanglement distillation. But Fig. 4(a) shows the positive effect of the deterministic Gaussian entanglement swapping protocol based QR, which outperforms direct transmission beyond distances of 350 km. At this crossover point the Gaussian swapping approach uses approximately 1000 EPR pairs.

D. NG entanglement swapping based CV QR

Now let us turn our attention to the NG entanglement swapping based CV quantum repeaters using the ideal system assumptions from the above apart from channel losses. Now while we must perform entanglement swapping operations at every nesting level, we do have the freedom to optimize over whether we perform distillation operations and if so which type. With these assumptions the key rates are plotted and compared with direct transmission in Figs. 4(b) and 4(c) for the NG swapping approaches, respectively. The dots correspond to the numerically optimized key rates and the curve is an interpolation through it. We see that the crossing point where the CV QR scheme performs better than direct transmission is near 500 km for the NG swapping operations compared with 350 km for the Gaussian swapping approach.

In the regime between 350 and 600 km the Gaussian swapping scheme is outperforming the NG swapping operation by two orders of magnitude but we need to be careful here. The displacement correction gates present in each Gaussian swapping operation tend to add higher photon number states to our resulting entangled states, which in turn moves those states outside the low photon number space required for the NG distillation. This forces us to start with an entangled source with reduced squeezing parameter λ (compared to the NG case). As our communication distance L increases we need to perform more swapping operations and in turn this means we need to decrease the squeezing parameter even further. We need to tune the strength of our entanglement source depending not only on the distance between adjacent repeater nodes but also on L . This is not ideal and means it is hard to guarantee a polynomial scaling for arbitrary communications distances. Further as we have more repeater stations we need to increase the number of Gaussification operations within each Gaussian swapping scheme. This in turn means the performance decreases further and the NG swapping operation approach is better.

E. Optimal strategies

In our previous subsections of this section, we have established that our CV quantum repeater EPR generation rate and resources consumed scale polynomial with the overcommunications distance. Further we have shown what potential normalized QKD key rates can be generated using both Gaussian and NG entanglement swapping based approaches. In both cases we determined the distance at which the repeater approach beats direct transmission.

We should now consider what the best performance strategy is at the various communication distances of interest.

(i) For distances below 350 km direct transmission (no repeater stations) is best, while for greater distances CV QRs are helpful (see Fig. 4).

(ii) For distances between 350 km and 10000 km the optimal strategy is to first distribute a state with very low squeezing ($\lambda \leq 0.05$) and apply a symmetric PR distillation to distill a state with Gauss parameter $\lambda_\infty \approx 1$. The reason is that for low squeezing the decrease in purity due to fiber losses can be minimized (a higher initial squeezing would result in a very mixed state after the distribution). Since our distributed state has high purity, it is not necessary to apply a purifying distillation protocol and a symmetric PR distillation is sufficient. Indeed, if the symmetric PR distillation is applied to boost the Gauss parameter to $\lambda_\infty \approx 1$, also the transmittance gets a boost to $\tau_\infty \approx 1$. The price we have to pay is simply a low success probability of our symmetric PR distillation, which is still favorable compared to applying additional purification. The fact that a low initial squeezing is beneficial in combination with symmetric PR distillation has already been noted in the context of Gaussian entanglement distillation [28].

(iii) For distances beyond 10000 km, a similar strategy to the previous one can be used except that we add one additional purifying distillation after the first swapping operation. We see in Fig. 4 that the obtained key rate is slightly lower than with no additional purification for the plotted distances. However, the gap becomes closer as the distance gets larger and finally, after about 10 000 km, a crossing is expected. Moreover, we expect that the previous strategy without additional purifying distillation may not allow distribution over arbitrary distances as the NG entanglement swapping will fail as soon as the Gauss parameter τ_∞ falls below a certain threshold (see Fig. 3).

In our simulation, we optimized over the initial, final, and intermediate Gauss parameter for the squeezing and the number of swapping operations. In Table I, we give example values of the optimal Gauss parameters for 1500 km and both strategies. We see that the final state distributed over the total distance using CV QR has much higher purity for the second strategy, but the success probability is lower. In both cases we see that the normalized key rate is relatively high, which implies that it is robust against finite-size effects and excess noise. Moreover, since the distributed states provide a high normalized key rate, the scheme is robust against finite-size effects. So, even for distances below 500 km our scheme proves to be useful for practical CV QKD. Typically, long distance CV QKD fails because the difference between Bob's and Eve's information about the key gets very small or even goes to zero if noise and finite-size corrections are considered. Hence long distance CV QKD is not robust against noise and finite-size effects. However, in our scheme with a repeater one can distribute a sufficiently entangled state so that in spite of finite-size effects and noise at the detectors a key can be distilled.

VIII. COMPARING CV AND DV QR'S

It is necessary with any CV quantum repeater to compare it to the discrete variable situation as we can always use the discrete quantum repeaters to generate a Bell pair between the end nodes. One can then use the Bell pair to teleport the weakly squeezed two-mode squeezed (EPR) state followed by Gaussification to make it more entangled and Gaussian-like.

TABLE I. Gauss parameters λ_∞ and τ_∞ at the different stages of the QR protocol as well as the success probability p_{succ} of the operations. The total distance is 1500 km and the values of the first three columns correspond to the strategy without purification, while the right three columns show the one with applying the purifying distillation. The initial state refers to the EPR state after distribution. We see that the first strategy needs only three swapping operations (seven repeater stations), while the optimal strategy with purification requires four swapping operations (15 repeater stations). We note that only a slightly lower key rate is obtained for the protocol with purification and only three swapping operations such that it might be favorable from a practical point of view. In the last swapping operation it is beneficial to decrease λ_∞ , which is favorable to a high normalized key rate $r(\sigma)$ if only two iterations of the Gaussification protocol are applied. The key rate $r_{\text{QR}}(\sigma)$ and the normalized key rate $r(\sigma)$ without (with) purification are 0.14 (0.27) and 2.3×10^{-14} (2.2×10^{-15}), respectively.

	λ_∞	τ_∞	p_{succ}	λ_∞	τ_∞	p_{succ}
Initial state	0.013	0.013		0.04	0.11	
PR dist.	0.95	0.99	6.5×10^{-8}	0.98	0.96	4.5×10^{-5}
First swap	0.95	0.97	0.027	0.98	0.93	0.028
Purification				0.98	0.995	2.5×10^{-3}
Second swap	0.9	0.94	0.028	0.98	0.99	0.028
Third swap	0.65	0.83	0.035	0.98	0.98	0.038
Fourth swap				0.55	0.91	0.038
Gaussification	0.65	0.83	0.093	0.55	0.91	0.11

To begin the comparison we need to think about the elements of our repeater's resources. In the CV regime we require a source of both two-mode squeezed states and ideal detectors (both CV and single photon based). The single photons required within the local nodes can be generated in a heralded fashion from the EPR states. Our resource count in this situation will be the number of EPR states sent through the channel. Now the important question is what are our DV components. We can use the EPR state as a probabilistic source of Bell pairs to be sent through the channel (the EPR state is weakly squeezed to minimize the two photon components).

Consider now a five node (Alice, Bob, and three immediate nodes)–four segment repeater network with each adjacent repeater node separated by 87.5 km (the total distance between Alice and Bob is 350 km). The probability of an ideal single photon to be transmitted over 87.5 km of telecom fiber is ~ 0.03 . Remembering the single photon comes from a weak EPR state (mean photon number of 0.03 say), the probability for generating a single link between adjacent nodes would be ~ 0.001 . Once these Bell pairs are stored within the repeater nodes we will perform one round of probabilistic but heralded purification (with success probability of 1/4) followed by a round of entanglement swapping (success probability of 1/2). We then purify the resulting swapped Bell pairs followed by a final round of entanglement swapping. The key question is how many Bell pairs do we need to generate our entangled link between Alice and Bob. To generate an average of one Bell pair, it is straightforward to show that on average 1024 Bell states are needed (256 between each set of nodes). This means we get a normalized rate per pulse $\sim 10^{-6}$. The rate will drop further by more than an order of magnitude as we

probabilistically teleport one-half of the $|00\rangle + q|11\rangle$ and then perform Gaussification. Finally, when one examines the CV situation as shown in Fig. 4(a), we observe that the 350 km total distance corresponds to the point where the Gaussian based entanglement swapping quantum repeater begins to outperform direct transmission. At this crossover point, the normalized rate per pulse is approximately 10^{-6} for the CV QR and is better than the equivalent DV QR mentioned above. However, we need to be very careful before making a definite conclusion as it is very hard to make a fair comparison.

IX. DISCUSSION AND CONCLUSION

In this work we have presented a CV QR scheme whose EPR generation rate and resources consumed scale polynomially with the total communications distance. The distributed entangled EPR states (with arbitrary squeezing and fidelity) can then be used for many CV communication applications such as quantum teleportation or CV QKD. Alternatively they can also be used for communicating DV quantum information used in a qubit based quantum computer [49]. We analyzed the performance of our protocol by examining its use in CV QKD (see Fig. 4) and found the crossing point, where the key rates with the CV QR are larger than with direct transmission, is near 350–550 km depending on the entanglement swapping scheme. By analyzing the key rate for larger distances, we observe the strong positive effect of the polynomial scaling. This is due to the fact that the purification protocol has a low success probability. Indeed the lower plot in Fig. 4 shows that the range where an application of the purifying distillation protocol is beneficial is beyond 10000 km. This illustrates one of the current problems of the CV QR, which is the low efficiency of the purifying entanglement distillation protocol. Compared to the entanglement increasing symmetric PR distillation, it has a success probability of about two to three magnitudes lower. Hence an important step in improving the proposed CV QR protocol is to find entanglement distillation protocols that increase the purity, but have a practical success probability. It is known that purification is not possible with simple heralded operations on only one mode [29]. But we still expect that under moderate increase of the experimental difficulty an improved purification scheme is possible.

This is not the only challenge that remains for CV QR; in fact, there are many of them. One of the most important is given in the situation where the final state has to be very close to a Gaussian EPR state. Since the Gaussification protocol is based on a noncommutative central limit theorem, we expect that the approximation error ϵ goes as $1/\sqrt{N}$, where N is the number of iterations. Hence, given the iterative scheme of the Gaussification protocol, the success probability scales exponentially in $1/\epsilon^2$. This problem could have been greatly avoided in our application to CV QKD, where a Gaussian state is not essential. But it is not clear how a NG or (badly) approximate Gaussian state performs in a Gaussian teleportation or Gaussian entanglement swapping protocol. This is also the reason why we only obtained a quantitative estimation if using the NG entanglement swapping protocol, and could only approximate the scaling of the CV QR with the Gaussian entanglement swapping protocol (see Fig. 4). However, since Gaussian entanglement swapping has the big

advantage of being deterministic, it is important to determine the approximation errors after a finite number of iterations of the Gaussification protocol and how such errors affect the output fidelity of the state after Gaussian entanglement swapping.

Even if all these issues are overcome, the performance of these CV QRs will be quite slow due to the long-range classical communication that is needed in the entanglement distillation steps. What we have designed here is analogous to the first generation DV QRs, which were also extremely slow [12,15,41]. Improvement in DV repeater design to second [50,51] and third [19,52,53] generations offered the potential for huge speed improvements. The second generation DV schemes replaced the traditional purification algorithms with full deterministic local node error corrections [50,51] and so their operational speed was limited by the communication times between adjacent nodes rather than the communication between the end nodes. Orders of magnitude increase in performance have been predicted [50,51]. The third generation DV QR went further and replaced the heralded entanglement distribution with a deterministic (or near deterministic) approach using photon loss coding [54,55]. The performance of such schemes were thus only limited by the gate times within the repeater nodes, and so GHz rates have been predicted [19,52,53]. If we can move the second and third generation DV QR concepts across to the CV QR, then we would expect large gains in our performance. This, however, requires the development of new CV error correction codes (both for gate errors and channel loss).

The main application we have discussed in this CV QR work is CV QKD and we have found in principle that the CV QR are an advantage in terms of communication rate once our users are more than 350 km apart. We must point out explicitly at this stage that our analysis assumed the only error arose from channel losses and further ignored finite-size effects. Further it is useful to emphasize, however, that our CV QR protocol should also be useful for CV QKD for lower distances. In practical implementations the distance of CV QKD is limited to less than 150 km due to finite-size effects and excess noise [14,21]. However, in our scheme with a CV QR one can distribute a sufficiently entangled state so that in spite of finite-size effects and noise at the detectors a key can be distilled. Thus the generated key rates from our scheme are practical and robust to such effects. Further an extension to an asymmetric entanglement distribution scheme for our CV QR protocol may further improve the distance.

Now to conclude, our CV QR scheme allows us to distribute entangled EPR states with an arbitrary fidelity over long distances that have a success probability scaling polynomial with distance. Further we have shown how the distributed states can be used for CV QKD with rates that exceed the ones by direct transmission. Our approach here has shown that CV QR are in principle possible and so we have assumed perfect single photon sources and detectors and not included the effect of realistic errors or noise (apart from channel loss). While we expect that our CV QR scheme is robust under small deviation of these assumptions, it is important to make this more precise in future work. In particular, the question whether single photon sources can be replaced by weak coherent states is crucial to allow for high-frequency CV QR implementations. This would provide a clear advantage over

DV QR approaches which often rely on true single photon sources.

ACKNOWLEDGMENTS

We gratefully acknowledge useful discussions with Jens Eisert, Akihito Soeda, Koji Azuma, and Kiyoshi Tamaki. This work was partially supported by the John Templeton Foundation (The Nature of Quantum Networks (ID 60478)).

APPENDIX: PURIFYING DISTILLATION DETAILS

Due to the importance of the purifying distillation, let us examine this scheme in more detail by characterizing the effect of the operation on the matrix elements in the number basis. These are computed by

$$\tilde{\rho}_{kl,\alpha\beta} = \langle k, l | D(q) \otimes D(q) (\rho \otimes \rho) D(q)^* \otimes D(q)^* | \alpha, \beta \rangle. \quad (\text{A1})$$

A straightforward calculation using (15) shows

$$D(q)^* | k \rangle = \sum_{l=-1}^k | k-l \rangle \otimes (q d_{k|l} | l \rangle + \tilde{d}_{k|l} | l+1 \rangle), \quad (\text{A2})$$

where

$$d_{k|l} = \gamma_k(q) \sum_{t=0}^k (k-t-1)(t-1) \alpha_{k0|t} \alpha_{(k-1)t|(l-t)}, \quad (\text{A3})$$

$$\tilde{d}_{k|l} = \gamma_k(q) \sum_{t=-1}^k \sqrt{\frac{1}{2}} t (k-t-1) \alpha_{k1|t} \alpha_{(k-t)(t+1)|(l-t)}, \quad (\text{A4})$$

with $\gamma_k(q) = (1/2)^{(k+1)/2} / \sqrt{1+q^2}$ and where we use the convention $d_{k|-1} = 0$. Let us now assume that $F_1(\rho)$ has the form in (6). This allows us to explicitly compute $\tilde{\rho}_{kl,\alpha\beta}$ and determine the coefficients of $F_1(\tilde{\rho})$ as

$$\rho_{00,00} = \frac{1}{2^2} \frac{q^4}{(1+q^2)^2} \rho_{00,00}^2, \quad (\text{A5})$$

$$\rho_{10,10} = \frac{1}{2^4} \frac{q^2}{(1+q^2)^2} \rho_{10,10}^2, \quad (\text{A6})$$

$$\rho_{01,01} = \frac{1}{2^4} \frac{q^2}{(1+q^2)^2} \rho_{01,01}^2, \quad (\text{A7})$$

$$\rho_{11,00} = \frac{1}{2^4} \frac{q^2}{(1+q^2)^2} \rho_{11,00}^2, \quad (\text{A8})$$

$$\rho_{11,11} = \frac{1}{2^{10}} \frac{1}{(1+q^2)^2} \rho_{11,11}^2, \quad (\text{A9})$$

with all the others being zero. Hence the structure of F_1 is conserved by the purifying distillation.

Numerical calculations further suggest that the condition (5) is conserved in general by the purifying distillation. Unfortunately, we were not able to prove this explicitly. However, for our CV QR it is sufficient that the structure of F_1 (6) is conserved, in order for the Gauss parameter to remain meaningful. This is because for all subprotocols $F_1(\tilde{\rho})$ is only a function of $F_1(\rho)$. Using the above formulas, we see that for the purifying distillation [29]

$$\varepsilon(\tilde{\rho}) = \varepsilon(\rho)^2. \quad (\text{A10})$$

Since for meaningful states $\varepsilon \leq 1$, we find that ε reduces with purifying distillation leading to a state with increased purity.

- [1] G. J. Milburn, *Schrödinger's Machines* (W. H. Freeman & Co., San Francisco, 1997).
- [2] J. P. Dowling and G. J. Milburn, *Philos. Trans. R. Soc. London A* **361**, 3655 (2003).
- [3] T. P. Spiller and W. J. Munro, *J. Phys.: Condens. Matter* **18**, V1 (2006).
- [4] H. J. Kimble, *Nature (London)* **453**, 1023 (2008).
- [5] R. Feynman, *Int. J. Theor. Phys.* **21**, 467 (1982).
- [6] D. Deutsch, *Proc. R. Soc. London A* **400**, 97 (1985).
- [7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [8] H.-K. Lo, M. Curty, and K. Tamaki, *Nat. Photon.* **8**, 595 (2014).
- [9] ID quantique, <http://www.idquantique.com>.
- [10] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache *et al.*, *Opt. Express* **20**, 14030 (2012).
- [11] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, *Opt. Express* **19**, 10387 (2011).
- [12] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, *Rev. Mod. Phys.* **83**, 33 (2011).
- [13] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Rev. Mod. Phys.* **84**, 621 (2012).
- [14] E. Diamanti and A. Leverrier, *Entropy* **17**, 6072 (2015).
- [15] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, *IEEE J. Sel. Top. Quantum Electron.* **21**, 6400813 (2015).
- [16] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **81**, 5932 (1998).
- [17] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, *Phys. Rev. A* **59**, 169 (1999).
- [18] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, *Nature (London)* **414**, 413 (2001).
- [19] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, *Nat. Photon.* **6**, 777 (2012).
- [20] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Sci. Rep.* **6**, 20463 (2016).
- [21] D. Huang, P. Huang, D. Lin, and G. Zeng, *Sci. Rep.* **6**, 19201 (2016).
- [22] R. Namiki, O. Gittsovich, S. Guha, and N. Lütkenhaus, *Phys. Rev. A* **90**, 062316 (2014).
- [23] J. Eisert, S. Scheel, and M. B. Plenio, *Phys. Rev. Lett.* **89**, 137903 (2002).
- [24] J. Fiurášek, *Phys. Rev. Lett.* **89**, 137904 (2002).
- [25] G. Giedke and J. I. Cirac, *Phys. Rev. A* **66**, 032316 (2002).
- [26] D. E. Browne, J. Eisert, S. Scheel, and M. B. Plenio, *Phys. Rev. A* **67**, 062320 (2003).
- [27] J. Eisert, D. E. Browne, S. Scheel, and M. B. Plenio, *Ann. Phys. (NY)* **311**, 431 (2004).
- [28] A. P. Lund and T. C. Ralph, *Phys. Rev. A* **80**, 032309 (2009).
- [29] J. Fiurášek, *Phys. Rev. A* **82**, 042331 (2010).
- [30] E. T. Campbell and J. Eisert, *Phys. Rev. Lett.* **108**, 020501 (2012).
- [31] E. T. Campbell, M. G. Genoni, and J. Eisert, *Phys. Rev. A* **87**, 042330 (2013).
- [32] J. Dias and T. C. Ralph, *Phys. Rev. A* **95**, 022312 (2017).
- [33] T. Ralph and A. Lund, in *Proceedings of the 9th International Conference on Quantum Communication Measurement and Computing*, edited by A. Lvovsky (AIP, New York, 2009), pp. 155–160.
- [34] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).
- [35] M. Dakna, J. Clausen, L. Knöll, and D.-G. Welsch, *Phys. Rev. A* **59**, 1658 (1999).
- [36] J. Hoelscher-Obermaier and P. van Loock, *Phys. Rev. A* **83**, 012319 (2011).
- [37] S. L. Braunstein and H. J. Kimble, *Phys. Rev. Lett.* **80**, 869 (1998).
- [38] T. C. Ralph and P. K. Lam, *Phys. Rev. Lett.* **81**, 5668 (1998).
- [39] L. Vaidman, *Phys. Rev. A* **49**, 1473 (1994).
- [40] Note that, due to our swapping and distillation protocol, we only set a minimal condition for the Gauss parameters determined by the target state. Hence the actual probability may slightly vary but can be bounded by optimizing over all states that comply with the target state.
- [41] R. Van Meter, T. D. Ladd, W. J. Munro, and K. Nemoto, *IEEE/ACM Trans. Netw.* **17**, 1002 (2009).
- [42] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin *et al.*, *Phys. Rev. A* **76**, 042305 (2007).
- [43] R. Garcia-Patron and N. J. Cerf, *Phys. Rev. Lett.* **97**, 190503 (2006).
- [44] M. Navascues, F. Grosshans, and A. Acin, *Phys. Rev. Lett.* **97**, 190502 (2006).
- [45] A. Leverrier, *Phys. Rev. Lett.* **114**, 070501 (2015).
- [46] R. Renner and J. I. Cirac, *Phys. Rev. Lett.* **102**, 110504 (2009).
- [47] F. Grosshans, G. van Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, *Nature (London)* **421**, 238 (2003).
- [48] P. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Nat. Commun.* **8**, 15043 (2017).
- [49] S. Takeda, T. Mizuta, M. Fuwa, P. van Loock, and A. Furusawa, *Nature (London)* **500**, 315 (2013).
- [50] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, *Phys. Rev. A* **79**, 032325 (2009).
- [51] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, *Nat. Photon.* **4**, 792 (2010).
- [52] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. L. Hollenberg, *Phys. Rev. Lett.* **104**, 180503 (2010).
- [53] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Phys. Rev. Lett.* **112**, 250501 (2014).
- [54] T. C. Ralph, A. J. F. Hayes, and A. Gilchrist, *Phys. Rev. Lett.* **95**, 100501 (2005).
- [55] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, *Rev. Mod. Phys.* **79**, 135 (2007).